



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|--------------------------|------------------|
| 10/019,012 | 12/26/2001 | Robert John Briscoe | 36-1518 | 5924 |
| 23117 | 7590 | 05/16/2006 | | |
| NIXON & VANDERHYE, PC 901 NORTH GLEBE ROAD, 11TH FLOOR ARLINGTON, VA 22203 | | | | |
| | | | EXAMINER BAUM, RONALD | |
| | | | ART UNIT 2136 | PAPER NUMBER |

DATE MAILED: 05/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|------------------------------|--------------------------------------|---|--|
| Office Action Summary | Application No. 10/019,012 | Applicant(s) BRISCOE, ROBERT JOHN | |
| | Examiner Ronald Baum | Art Unit 2136 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 March 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>05092006</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 01 March 2006.
2. Claims 1-25 are pending for examination.
3. Claims 1-25 remain rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-25 are rejected under 35 U.S.C. 102(b) as being anticipated by Kambayashi et al, U.S. Patent 6,477,649 B2.

5. As per claim 1; "A method of distributing data comprising:

(a) encrypting a plurality of data units each with

one of a sequence of keys [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method where the multimedia content clearly is formatted in a plurality of data units, and encryption at a per key per unit information, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

(b) communicating encrypted data units to

a plurality of user terminals [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that content is broadcast to reception terminals, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

(c) communicating at least one seed value to

a user terminal [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key generation/regeneration information (i.e., the key seed) is broadcast to reception terminals, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

(d) generating from the seed value or values

a sequence of keys greater in number than

the number of seed values communicated to the user terminal [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the key seed at the reception terminals is clearly greater than the number of seed(s), and clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

(e) decrypting data units at the user terminal using

the said sequence of keys, characterized

in that in step (d) a sequence of keys constituting an arbitrarily doubly bounded portion of the sequence of keys of step (a) is generated, and

in that the position in sequence of the lower and upper bounds of the said portion are determined by the at least one seed value communicated in step (c) [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the key seed at the reception terminals is such that the inclusive user/content identification/licensing information as applied to the seed key regeneration clearly produces a user terminal subset of the entire key space, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.].”.

6. Claim 2 ***additionally recites*** the limitation that; “A method according to claim 1, in which the sequence of keys used in step (a) is generated by:

(a)

operating on one or more initial seed values and

generating a greater number of intermediate seed values, which intermediate seed values

blind the initial seed values:

(b) further

operating on the values produced by the preceding step and

generating thereby a still greater number of further values, which further values

blind the values produced by the preceding step;

(c) iterating step (B) until

the number of values produced is equal to or greater than

the number of keys required for step (a).”.

The teachings of Kambayashi et al suggest such limitations (i.e., figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the initial key seed at the reception terminals is a function of multiple cryptographic algorithms, inclusive of hashing (i.e., blinding) functions, whereas the functions are clearly iterative (i.e., figures 134-138) and therefore producing intermediate seeds/keys, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

7. Claim 3 ***additionally recites*** the limitation that; “A method according to claim 1, in which step (d) includes

combining values derived from

a plurality of different seed values.”.

The teachings of Kambayashi et al suggest such limitations (i.e., figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the initial key seed at the reception terminals is a function of

Art Unit: 2136

multiple cryptographic algorithms, inclusive of hashing (i.e., blinding) functions, whereas the functions are clearly iterative (i.e., figures 134-138) and therefore producing intermediate seeds/keys via the plurality of different seed values, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

8. Claim 4 *additionally recites* the limitation that; “A method according to claim 1, in which step (d) includes

operating on

a plurality of seed values with each of

a plurality of different blinding functions.”.

The teachings of Kambayashi et al suggest such limitations (i.e., figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the initial key seed at the reception terminals is a function of multiple cryptographic algorithms, inclusive of hashing (i.e., plurality of different blinding functions) functions, whereas the functions are clearly iterative (i.e., figures 134-138) and therefore producing intermediate seeds/keys via the plurality of different seed values, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

9. Claim 5 *additionally recites* the limitation that; “A method according to claim 4, including:

(I) operating on

at least one root seed value with each of
a set of different blinding functions thereby producing a plurality of
further values;
(II) operating with
each of the set of different blinding functions on
the further values produced by
the preceding step or
on values derived therefrom;
(III) iterating step (II) and thereby producing, by the or each iteration,
a next successive layer in a tree of values;
(IV) in step (a), using as the sequence of keys
values derived from the sequence of seeds in one or more of the layers produced
by step (III); and
(V) in step (c), communicating to a user terminal
at least one value from within the body of the tree,
the position in the tree of the or each value communicated to the user
terminal thereby determining
the position and
extent of the portion of the sequence of keys available to
the user for use in decrypting data units.”.

The teachings of Kambayashi et al suggest such limitations (i.e., figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information

Art Unit: 2136

content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the initial key seed at the reception terminals is a function of multiple cryptographic algorithms, inclusive of hashing (i.e., plurality of different blinding functions) functions, whereas the functions are clearly iterative (i.e., figures 134-138) and therefore producing intermediate seeds/keys via the plurality of different seed values, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

10. Claim 6 *additionally recites* the limitation that; "A method according to claim 5 including, in step (1)

(i) operating with

the set of different blinding functions on
plurality of different seed values

(ii) for each of the different blinding functions,

combining

the result of operating with

one blinding function on one of the seed values and

the result of operating with

the same or another blinding function on another of the respective

seed values, thereby producing

a plurality of further values."

The teachings of Kambayashi et al suggest such limitations (i.e., figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information

Art Unit: 2136

content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the initial key seed at the reception terminals is a function of multiple cryptographic algorithms, inclusive of hashing (i.e., plurality of different blinding functions) functions, whereas the functions are clearly iterative (i.e., figures 134-138) and therefore producing intermediate seeds/keys via the plurality of different seed values, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

11. Claim 7 *additionally recites* the limitation that; “A method according to claim 3, in which step (d) includes

(I) combining

first and second values derived from respective

first and second blinding function chains, thereby producing

a first next seed or key, the first and second blinding function chains

having different respective seeds

(II) combining

a value derived from

a position in the first chain subsequent to

the position of the first value and

a value derived from

a position in the second chain preceding

the position of the second value, thereby producing

a further next seed or key value.”.

Art Unit: 2136

The teachings of Kambayashi et al suggest such limitations (i.e., figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the initial key seed at the reception terminals is a function of multiple cryptographic algorithms, inclusive of hashing (i.e., plurality of different blinding functions) functions, whereas the functions are clearly iterative (i.e., figures 134-138) and therefore producing intermediate seeds/keys via the plurality of different seed values, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

12. Claim 8 *additionally recites* the limitation that; "A method according to claim 7, including

iterating step (II) thereby producing further key values, in each iteration
values from positions
subsequent to the previous position in the first chain and
preceding the previous position in the second chain
being combined."

The teachings of Kambayashi et al suggest such limitations (i.e., figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the initial key seed at the reception terminals is a function of multiple cryptographic algorithms, inclusive of hashing (i.e., plurality of different blinding functions) functions, whereas the functions are clearly iterative (i.e., figures 134-138) and

Art Unit: 2136

therefore producing intermediate seeds/keys via the plurality of different seed values, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

13. Claim 9 *additionally recites* the limitation that; “A method according to claim 1 in which the seed values are communicated to

the user terminals, via a communications network.”.

The teachings of Kambayashi et al suggest such limitations (i.e., figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key generation/regeneration information (i.e., the key seed) is broadcast to reception terminals over various network configurations, and therefore clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

14. Claim 10 *additionally recites* the limitation that; “A method according to claim 9 in which

the seed values are communicated from

a plurality of key management nodes to customer terminals. ”.

The teachings of Kambayashi et al suggest such limitations (i.e., figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key generation/regeneration information (i.e., the key seed) is broadcast to reception terminals over various network configurations, inclusive of intermediate nodes (i.e.,

Art Unit: 2136

key management server node to customer client terminals), and therefore clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

15. Claim 14 *additionally recites* the limitation that; “A method according to claim 1, in which

each encrypted data unit carries

an unencrypted index number to

identify to any receiver which key in the sequence should be used to

decrypt that data unit.”.

The teachings of Kambayashi et al suggest such limitations (figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution (i.e., unencrypted index information to identify receiver reception terminals)/reproduction apparatus and associated method where the multimedia content clearly is formatted in a plurality of data units, and encryption at a per key per unit information, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

16. Claim 15 *additionally recites* the limitation that; “A method according to claim 1 where the seeds required by any receiver to construct the keys for a specific sub-range of the entire key sequence are

communicated in an order that implicitly identifies each seed.”.

The teachings of Kambayashi et al suggest such limitations (i.e., figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information

Art Unit: 2136

content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the initial key seed at the reception terminals is a function of the licensing/user specific, and therefore destination specific, and implicitly identifying each seed, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

17. Claim 16 *additionally recites* the limitation that; "A method according to claim 1, in which

multiple data senders use the same sequence of keys as each other to
encrypt the same or different data units."

The teachings of Kambayashi et al suggest such limitations (figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information (same sequence of keys as each other) content recording/distribution (multiple data senders)/reproduction apparatus and associated method such that content is broadcast to reception terminals, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

18. Claim 17 *additionally recites* the limitation that; "A method according to claim 1, in which

each key in the sequence generated from the seeds is used as
an intermediate key to be combined with
another intermediate key or sequence of keys to produce
a sequence of keys to encrypt or decrypt the data units."

Art Unit: 2136

The teachings of Kambayashi et al suggest such limitations (figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key generation via the key seed at the source is such that the inclusive user/content identification/licensing information as applied to the seed key generation clearly produces a intermediate key to be combined with iteratively generated intermediate key or sequence of keys, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

19. As per claim 22, this claim is the apparatus for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection, as such; "A communications network comprising

means arranged to operate by method in accordance with the method of claim 1."

20. Claim 23 *additionally recites* the limitation that; "A network according to claim 22, in which

the data is distributed using

a multicast or

broadcast transmission mode."

The teachings of Kambayashi et al suggest such limitations (figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that content is

Art Unit: 2136

broadcast to reception terminals, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

21. Claim 24 *additionally recites* the limitation that; “A network according to claim 22,
in which the network includes
a virtual private network (VPN) and
in which different combinations of seeds for constructing different sub-ranges of keys for
decrypting data
give members of the virtual private network
different periods of access to the VPN.”.

The teachings of Kambayashi et al suggest such limitations (figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that content is broadcast across the Internet, or the like, to reception terminals, of which such Internet paths are inclusive of secure pathways (i.e., VPN's/Ipsec, etc.), and clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

22. As per claim 25, this claim is the apparatus for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection, as such; “A data carrier storing a plurality of data units encrypted for use in
a method according to claim 1.”.

Art Unit: 2136

23. As per claim 11; "A method of encrypting data for distribution comprising:

(a) operating on

at least one root seed value with

one or more blinding functions, thereby producing a plurality of further values

[figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the key seed at the reception terminals is a function of multiple cryptographic algorithms, inclusive of hashing (i.e., blinding) functions, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

(b) operating with

one or more blinding functions on

the further values produced by the preceding step or on values derived therefrom

[figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the key seed at the reception terminals is a function of multiple cryptographic algorithms, inclusive of hashing (i.e., blinding) functions, whereas the functions are clearly iterative (i.e., figures 134-138), and clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

(c) iterating step (b) and thereby producing, by the or each iteration,

a next successive layer in a tree of values [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the key seed at the reception terminals is a function of multiple cryptographic algorithms, inclusive of hashing (i.e., blinding) functions, whereas the functions are clearly iterative (i.e., figures 134-138), and clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

(d) encrypting

a plurality of data units using

a sequence of key values derived from

one or more of the layers generated by step (c) [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method where the multimedia content clearly is formatted in a plurality of data units, and encryption at a per key per unit information, clearly encompasses the claimed limitations as broadly interpreted by the examiner.].”.

24. As per claim 12; “A method of communicating data to a group of users comprising:

(a) encrypting data for distribution [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method where the multimedia

Art Unit: 2136

content and broadcast to multiple reception terminals, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

(b) systematically and independently of group membership changes

changing a key used in encrypting the data for distribution [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the key seed at the reception terminals is such that the inclusive user/content identification/licensing information as applied to the seed key regeneration clearly produces a user terminal subset of the entire key space, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

(c) communicating the data to the users [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that content is broadcast to reception terminals, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

(d) at the users' terminals

decrypting the data, characterized by generating from

a number of initial seed values

a greater number of intermediate seed values, and

deriving from the intermediate seed values

the plurality of keys used in encrypting the data for distribution [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the key seed at the reception terminals is such that the inclusive user/content identification/licensing information as applied to the seed key regeneration clearly produces a user terminal subset of the entire key space, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.].”.

25. Claim 13 *additionally recites* the limitation that; “A method according to claim 12, in which

every possible subset of the sequence of keys is derivable from
a respective combination of seed values.”.

The teachings of Kambayashi et al suggest such limitations (figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the key seed at the reception terminals is such that the inclusive user/content identification/licensing information as applied to the seed key regeneration clearly produces a user terminal subset of the entire key space, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

Art Unit: 2136

26. As per claim 18; "A method of distributing data comprising
encrypting a plurality of data units each with
one of a sequence of keys and
communicating the encrypted data units to
a plurality of user terminals, characterized
in that the sequence of keys is generated and allocated to application data
units in accordance with a key construction algorithm, and
in that copies of the key construction algorithm are distributed to
a plurality of key managers so that, in use, receivers may
obtain keys for access to an arbitrary portion of the data
from
a key manager without reference to
any data sender or senders [figures 111-140 and
associated descriptions, whereas the use of a seed/key
based cryptographic security/licensing information content
recording/distribution/reproduction apparatus and
associated method such that cryptographic key regeneration
via the key seed at the reception terminals is such that the
inclusive user/content identification/licensing information
as applied to the seed key construction algorithm(s) clearly
produces a user terminal subset of the entire key space at
various network nodes (plurality of key managers), and

clearly encompasses the claimed limitations as broadly interpreted by the examiner.].”.

27. As per claim 20, this claim is the means plus function for the method claim 18 above, and is rejected for the same reasons provided for the claim 18 rejection, as such; “A key manager comprising

means arranged to operate in accordance with the method of claim 18.”.

28. As per claim 19; “A method of operating a user terminal comprising:

a) receiving

a plurality of data units encrypted with

a sequence of keys [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method where the multimedia content clearly is formatted in a plurality of data units, and encryption at a per key per unit information, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

b) receiving

one or more seed values [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key generation/regeneration information (i.e., the key seed) is broadcast to

Art Unit: 2136

reception terminals, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

c) generating from the one or more seed values

an arbitrarily doubly bounded key sequence larger in number than

the number of seeds received in step (b) [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key generation/regeneration information (i.e., the key seed) is broadcast to reception terminals, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

d) decrypting

the application data units using

the values generated in step (c) or values derived therefrom [figures 111-140 and associated descriptions, whereas the use of a seed/key based cryptographic security/licensing information content recording/distribution/reproduction apparatus and associated method such that cryptographic key regeneration via the key seed at the reception terminals is such that the inclusive user/content identification/licensing information as applied to the seed key regeneration clearly produces a user terminal subset of the entire key space, and clearly encompasses the claimed limitations as broadly interpreted by the examiner.].”.

Art Unit: 2136

29. As per claim 21, this claim is the means plus function for the method claim 19 above, and is rejected for the same reasons provided for the claim 19 rejection, as such; "A customer terminal comprising

means arranged to operate in accordance with the method of claim 19."

Response to Amendment

30. As per applicant's argument concerning the lack of teaching by Kambayashi et al of a sequence of keys effectively used for encryption of a sequence of units of information, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive. The claim language (i.e., independent claim 1) is not directed to a sequence of unique keys, let alone the use of said keys on distinct information units in an explicit manor, just implicitly in a broad sense. The fact that the specification deals more explicitly with a sequence of unique keys does not render the requirement that the claim language not deal with this aspect more succinctly; just that said claim language is looked at in light of the specification. Therefore, the keys aspects of Kambayashi et al, consisting of a sequence of as few as a single key, used to encrypt multiple information units, as being *broadly interpreted by the examiner*, as per the claim language, would therefore be applicable in the rejection, such that said reference does not render the claim language limitations patently distinct.

31. As per applicant's argument concerning the lack of teaching by Kambayashi et al of generating more keys than the number of seeds transferred, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive. In the case of a single unique seed generated and transferred to multiple stations (i.e., network nodes), the keys generated at the nodes inherently are so generated subsequently at the nodes properly addressed to receive the said seeds (i.e., the key so generated is inherently a function of the seed value and the fact that a legitimate node can/does generate the key from the seed). The fact that the specification deals with the more explicit case of ignoring the addressed target of the site of key

Art Unit: 2136

generation of a particular seed(s) without consideration of the target addressed node as a parameter in the key generation does not render the requirement that the claim language not deal with this aspect more succinctly; just that said claim language is looked at in light of the specification. Therefore, the generating more keys than the number of seeds transferred aspects of Kambayashi et al, consisting of a sequence of as few as a single seed, used for multiple addressed target nodes for said seed reception, as being *broadly interpreted by the examiner*, as per the claim language, would therefore be applicable in the rejection, such that said reference does not render the claim language limitations patently distinct.

32. As per applicant's argument concerning the lack of teaching by Kambayashi et al of a pseudo-random "sequence" of numbers generated versus a random number, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive. The generation of true random numbers is clearly beyond the scope of the Kambayashi et al reference such that the generation is in fact a pseudo-random number per se, no matter what the reference refers to, as is clearly known in the art. The fact that the specification deals more explicitly with a pseudo-random "sequence" does not render the requirement that the claim language not deal with this aspect more succinctly; just that said claim language is looked at in light of the specification. Therefore, the pseudo-random "sequence" of numbers generated versus a random number, aspects of Kambayashi et al, as being *broadly interpreted by the examiner*, as per the claim language, would therefore be applicable in the rejection, such that said reference does not render the claim language limitations patently distinct.

Art Unit: 2136

33. As per applicant's argument concerning the lack of teaching by Kambayashi et al of bounded sequence, let alone a arbitrarily double bounded sequence, the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive. The use of any "arbitrary" (i.e., even a single key as a sequence of one) sequence as a predetermined sequence (again, even for the case of a single element) would inherently be double bounded as related to the sequence as so recited in the claim 1, as being *broadly interpreted by the examiner*, and does not render the claim language limitations patently distinct.

34. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2136

Conclusion

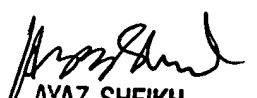
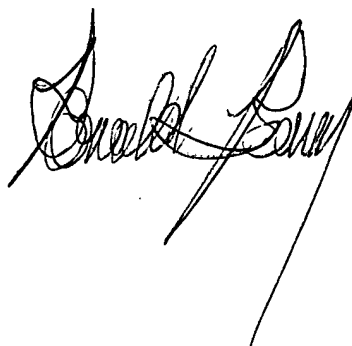
35. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100